WRITTEN STATEMENT

of

ART BOTTERELL
Emergency Information Systems Consultant

on

Public Safety Communications from 9/11 to Katrina: Critical Public Policy Lessons

Before the
Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
United States House of Representatives

29 September 2005

Good afternoon, Mr. Chairman and distinguished members of the Committee. My name is Art Botterell and I am an independent consultant on public warning and emergency information systems.

In my career in emergency communications I've served in public safety and government at the municipal, county, state and federal levels, and as a consultant and advisor in Asia and Europe. I've also been involved in international standards development for emergency data exchange, and in advocacy for improvements in public warning and emergency public information.

It's been my good fortune to accumulate first-hand experience with a wide array of emergency communications technologies and practices, and it's a privilege to share a few of the patterns I've detected with you here today.

Introduction: The Four Layers of Communication

Obviously the number one problem identified after 9/11 and again after the Katrina response was "communications." But what does that really mean?

For many years I've used a four-tiered "layer cake" model to help tease apart the various issues that get lumped under the broad rubric of "communication problems" or, more recently, "interoperability":

Organization	Structures, goals, objectives and metrics
Human Factors	Capabilities, training, stresses, personal attitudes
Procedures	Patterns of interaction and problem solving
Technologies	All the hardware, software and networks

(There's actually a fifth layer on top—Culture—which in most tactical contexts is a constant, but which definitely comes into play in cross-cultural and international applications.)

Over time I noticed two things about this formulation: The first was that problems, or at least the perceptions of problems, tend to propagate downward through the stack… so that a lot of non-technical issues wind up being framed as technology failures. The political or bureaucratic benefits of this depersonalized reframing are fairly clear, as is its attractiveness to vendors and other technology proponents, but it leads to a lot of what might be called "Groundhog Day" experiences, as succeeding generations of technology are blamed for the same breakdowns.

In two decades of emergency response field operations, I can truthfully say that I cannot recall any occasion when I felt the available technology was being fully utilized. In almost every case, I found it possible to substantially enhance the performance of communications by interventions at the procedural, human-factors or organizational levels.

The other interesting thing, which I came to appreciate more slowly, was that change tends to propagate upward through the stack. New technologies require and enable new behaviors, requiring new skills and triggering new stresses, and creating new forces to which organizations ultimately adapt themselves. This is a continual evolutionary process, and that has important implications to which I'll return in just a moment.

For now, the first insight is that a lot of the interoperability and data-sharing challenges we face aren't technical problems, and just painting over them with a fresh layer of technology won't necessarily solve them.

Prices We Don't Need to Pay

A couple of truisms here: Nothing is so permanent as a temporary solution, and nothing takes longer than a quick fix. Having been through these review exercises after just about every major disaster of the past two decades, I'll suggest that there are some things that we as a nation cannot—and need not—afford anymore. I'll suggest answers in a moment, but allow me a moment to review the problems first.

First, we can no longer afford to build separate infrastructure for different modes of communications. The question isn't radio versus computers, or voice versus data, or wired versus wireless. The question is how we can complete the process of digital convergence to get the most capability and reliability for all modes of emergency communication.

Second, we can no longer afford to treat the radio spectrum as, effectively, private property. We have much more efficient ways of separating, securing and identifying communications channels than by the fixed allocation of blocks of spectrum to either public or private licensees or services. Certainly this transition from the traditional approach will take time, and it will have financial implications, but the sooner we start the sooner we'll realize the benefits of dynamic spectrum management.

Third, we can no longer afford to rely on vendor-driven design of our emergency communications infrastructure. I make no criticism here of business doing business. The problem arises when government fails in its complementary role as steward of public

resources and champion for the public interest, thus leaving the competitive forces of the marketplace unchallenged and unconstrained by any higher values. The phenomenon of government program managers whose mastery of technologies is limited to what their contactors tell them is, alas, a commonplace of federal and, increasingly, of state and local government. Businesses are responsible for maximizing shareholder value, not for maximizing the general public welfare. We need independent sources of information and planning for our future emergency infrastructure, else we'll continue to get updated versions of the same old thing.

And finally, we can no longer afford an intermittent series of post-disaster quick-fix programs for emergency communications. Emergency managers are sadly aware of the "window of opportunity" for funding and legislative interest that opens, all too briefly, after every major disaster. It forces them to undertake impulsive, piecemeal procurements of whatever can be delivered quickly, because they know if they don't move quickly they'll soon be back near the bottom of the spending priorities list. The development of telecommunications is, as I've mentioned, a continual process of incremental improvement. It requires a consistent program of implementation as well.

So how might such a program be established?

How to Fix It

The first task is to frame the problem properly. The problem isn't just technical facilities; it's also procedures, human resources and organizational structures. We need to involve social scientists, economists and human factors engineers as well as electrical engineers and computer scientists. The goal isn't increased communication or enhanced information sharing; those are means, not ends. The goal is to increase the resilience and

robustness of our society and our economy, even as increasing efficiencies squeeze out the slack resources we used to count on to buffer us against unexpected events.

The second task is to learn three lessons from the Internet:

- **The "end-to-end principle"**—Simply put, this holds that the network should be as simple and transparent as possible, so applications and features can be negotiated and improved over time by the end users. (One implication of this is a distinction between the "user interface," e.g., a handheld radio, and the underlying network, which might be of various types without the user noticing any difference.)
- **The power of judicious standards**—The Internet has no architecture. Instead, the Internet is the spontaneous expression of a fairly simple set of enabling technical interface standards, upon which a rich and agile ecology of commercial and non-commercial innovation have been built, continually and incrementally. Likewise, the challenge for designing emergency communications capabilities is not to develop a global top-down architecture, but rather to identify and promote the key enabling standards that will allow technologies to interact, cooperate, compete and improve for the benefit of investors and the general public alike.
- **The revolution in standards development**—One quiet impact of the Internet has been on the processes by which technical standards are developed. The process used by the Internet Engineering Task Force stresses open participation, open non-proprietary interfaces, and a requirement that standards must actually have been implemented and

tested by multiple users prior to formalization. This open, iterative approach to standards development has spread to other standards organizations, and the result has been better, more robust standards being brought to use faster than by more traditional industry standards processes.

The third task is to learn how to harness the energies of the academic, volunteer and Open Source communities. It's been said that "Free is the one price government doesn't know how to pay." I've watched several generations of communications volunteers develop and demonstrate innovative and useful communications technologies, only to be frustrated by government bureaucracies that only knew how to adopt technologies by means of lengthy and complicated commercial procurement processes.

The highly successful open standard called the Common Alerting Protocol is one of the few such non-commercial initiatives that have broken through this bureaucratic glass ceiling. "CAP," as it's called, offers a pattern for harnessing the creative energy of the academic and open-source communities for the public good. Of course, success has a thousand fathers, and so I hope the process that led to the creation of CAP will be studied carefully before its product is fully absorbed into common process.

The Federal Government's Role

The federal government can play a key role in this process. The federal government can stimulate the development and adoption of open, non-proprietary technical standards by encouraging procurements requiring such standards through its grants to state and local agencies and its own procurements.

The federal government can also support independent research and educational outreach though academic and non-profit organizations, so that officials at all levels of government are no longer so dependent on vendors for information about communications and information technology options and trends.

And the federal government can provide micro-grants, counseling, recognition and other support for volunteer, academic, non-commercial and open-source innovators—through the Small Business Administration, perhaps—to help them push their good ideas across the gap into broader use.

Most importantly, the federal government can expand its leadership role in approaching the robustness, reliability and adaptability of our national communications infrastructure as a continual process of improvement, with discrete year-by-year goals and objectives, and in tearing down some of the traditional barriers—between disciplines and agencies, between voice and data, between emergencies and day-to-day—that have kept us from applying the lessons that disasters teach us time and again.

I would be pleased to respond to your questions.

Summary of Key Points

- Discussions of "communications" must include procedural, human-factors and organizational aspects as well as technology.
- Convergence means moving beyond separate voice, data, other networks.
- Radio frequency spectrum can managed dynamically more efficiently than by the traditional fixed allocation methods.
- Design and planning of emergency communications infrastructure cannot be left entirely to vendors or contractors.
- Development of emergency communications infrastructure must be continual, not done in fits and spurts after every disaster.
- Problem is robustness and adaptability; interoperability is a means to that end.
- The Internet teaches important lessons:
    - The "end-to-end principle" maximizes flexibility and adaptability
    - A few open standards can enable competition and continual improvement
    - Standard setting is faster and more realistic as it is more open
- The "glass ceiling" that keeps voluntary and open-source efforts from being brought into practice must be removed; the OASIS Common Alerting Protocol offers an example of how that process can work better.
- Government can:
    - Drive adoption of open standards through grant guidance and procurements;
    - Support independent research and user education;
    - Facilitate small ventures, academics and the open-source community in bringing innovation to the field; and,
    - Define a process of constant improvement for a robust national communications infrastructure.